CarrierAccess

Adit 3200

USER MANUAL

Part Number: 770-0156 BA
Product Release: 1.6
September 2007

Copyright 2007 Carrier Access Corporation. All rights reserved.

The information presented in this manual is subject to change without notice and does not represent a commitment on the part of Carrier Access Corporation. The hardware and software described herein are furnished under a license or non-disclosure agreement. The hardware, software, and manual may be used or copied only in accordance with the terms of this agreement. It is against the law to reproduce, transmit, transcribe, store in a retrieval system, or translate into any medium - electronic, mechanical, magnetic, optical, chemical, manual, or otherwise - any part of this manual or software supplied with the Adit 3200 for any purpose other than the purchaser's personal use without the express written permission of Carrier Access Corporation.

The Carrier Access logo and Adit are registered trademarks of Carrier Access Corporation. All other brand or product names are trademarks or registration trademarks of their respective companies or organizations.

Contact Information:

Carrier Access Corporation
5395 Pearl Parkway
Boulder, CO 80301-2490
Corporate Phone: (303) 442-5455
Fax: (303) 443-5908
www.carrieraccess.com

Customer Support Direct: (800) 786-9929
E-mail: tech-support@carrieraccess.com

PREFACE

Compliance

Safety of Information Technology Equipment

The Adit 3200 is safety certified by Underwriters Laboratories and is compliant with the following safety standards for information technology equipment:

- UL 60950-1
- CSA 60950-1

FCC Requirements, Part 15

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the Federal Communications Rules. These limits are designed to provide reasonable protection against harmful interference when equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at the user's own expense.

FCC Requirements, Part 68

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the rear panel of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. If requested, this number must be provided to the telephone company.

FCC Registration Number:	US: 2Z6ISNAN675849
Service Center in the USA:	Carrier Access Corporation 5395 Pearl Parkway Boulder, CO 80301-2490

The Facility Interface Code (FIC) associated with each private line application represents the type of service that will be provided by the telephone company. The following are currently registered:

Port:	FIC:	SOC:	Jack:
T1 1.544Mbps	04DU9-BN	6.0N	RJ48C
T1 1.544Mbps	04DU9-DN	6.0N	RJ48C
T1 1.544Mbps	04DU9-1KN	6.0N	RJ48C
T1 1.544Mbps	04DU9-1SN	6.0N	RJ48C

Plug and Jack Statement
A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See installation instructions for details.

Ringer Equivalence Number (REN)
The assignment of a Ringer Equivalence Number (REN) is not applicable for this device.

If the Adit 3200 causes harm to the telephone network, the telephone company will notify you in advance. If advance notice proves impractical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe such action is necessary.

The telephone company may make changes in its facilities, equipment operations, or procedures that could affect the operation of the Adit 3200. If this occurs, the telephone company will provide advance notice so that you may make necessary modifications to maintain uninterrupted service.

If you experience trouble with the Adit 3200, please first contact the distributor or dealer from which you purchased the product and then, as a second point of contact, contact Carrier Access Corporation for repair and/or warranty information.

If the trouble is causing harm to the telephone network, the telephone company may request that you remove the Adit 3200 from the network until the problem is resolved. User repairs must not be made. Doing so will void the warranty.

Do not install the Adit 3200 on public coin service provided by the telephone company. Connection to Party Line service is subject to state tariffs. (Contact your state public utilities commission for further information.)

To minimize damage caused by local lightning strikes and other electrical surges, it is recommended that the customer install an AC surge arrestor in the AC outlet to which the Adit 3200 is connected.

Industry Canada ICES-003

English
This class A digital apparatus complies with Canadian ICES-003.

French
Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Industry Canada CS-03

Registration Number: IC: 2638A-675849

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

The assignment of a Ringer Equivalence Number (REN) is not applicable for this device.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telephone company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alternations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

CAUTION! **USERS SHOULD NOT ATTEMPT TO MAKE SUCH CONNECTIONS THEMSELVES, BUT SHOULD CONTACT THE APPROPRIATE ELECTRIC INSPECTION AUTHORITY, OR ELECTRICIAN, AS APPROPRIATE.**

Safety Information

CAUTION! ALWAYS USE CAUTION WHEN INSTALLING TELEPHONE LINES. READ THE CAUTIONS BELOW FOR DETAILS ON SAFETY GUIDELINES TO PREVENT INJURY.

- **Never touch uninsulated telephone wires and terminals** unless the telephone line has been disconnected at the Network Interface (NI) as voltage potentials as high as 300 VAC may be present across the transmit and receive pairs
- **Only use No. 26 AWG or larger** telecommunication line cord, to reduce the risk of fire
- Never install telephone wiring during a lightning storm
- **Never install telephone jacks in wet locations** unless the jack is specifically designed for wet locations
- Refer to the installation section of this manual for a safe and proper installation procedure. All wiring external to this equipment should follow the current provision of the National Electrical Code

Notices

This manual contains important information and warnings that must be followed to ensure safe operation of the equipment.

DANGER! A *DANGER* NOTICE INDICATES THE PRESENCE OF A HAZARD THAT CAN OR WILL CAUSE DEATH OR SEVERE PERSONAL INJURY IF THE HAZARD IS NOT AVOIDED.

CAUTION! A *CAUTION* NOTICE INDICATES THE POSSIBILITY OF INTERRUPTING NETWORK SERVICE IF THE HAZARD IS NOT AVOIDED.

WARNING! A *WARNING* NOTICE INDICATES THE POSSIBILITY OF EQUIPMENT DAMAGE IF THE HAZARD IS NOT AVOIDED.

NOTE: A *Note* indicates information to help you understand how to perform a procedure or how the system works. Notes should be read before performing the required action.

Electrostatic Discharge (ESD) Precautions

ESD can damage processors, circuit cards, and other electronic components. Always observe the following precautions before installing a system component.

1. Do not remove a component from its protective packaging until ready to install.
2. Wear a wrist grounding strap and attach it to a metal part of the system unit before handling components. If a wrist strap is not available, maintain contact with the system unit throughout any procedure requiring ESD protection.

WARNING! INTEGRATED CIRCUITS (ICS) ARE EXTREMELY SUSCEPTIBLE TO ELECTROSTATIC DISCHARGE. UNLESS YOU ARE A QUALIFIED SERVICE TECHNICIAN WHO USES TOOLS AND TECHNIQUES THAT CONFORM TO ACCEPTED INDUSTRY PRACTICES, DO NOT HANDLE ICS.

The ESD warning label appears on packages and storage bags that contain static-sensitive products and components.

Warranty

Carrier Access warrants to BUYER that Product Hardware will be free from substantial defect in material and workmanship under normal use in accordance with its Documentation and given proper installation and maintenance for period of five years from the date of shipment by Carrier Access.

Carrier Access warrants that the Licensed Software, when used as permitted under its License Terms and in accordance with the instructions and configurations described in the Documentation (including use on Carrier Access product or a computer hardware and operating system platform supported by Carrier Access), will operate substantially as described in the Documentation for a period of ninety (90) days after date of shipment of the Licensed Software to BUYER.

This warranty shall not apply to Products or Software that have been either resold or transferred from BUYER to any other party. Any such transfer voids the above warranty and related licenses. Carrier Access offers expanded product care beyond what is covered by the warranty through different support plans. The plans are designed to maximize network availability through advance replacement for defective equipment. Please contact your Carrier Access representative for support program details.

Warranty Procedure

BUYER must promptly notify Carrier Access of any defect in the Product or Software and comply with Carrier Access' return/repair policy and procedures. Carrier Access or its agent will have the right to inspect the Product or workmanship on BUYER's premises. With respect to a warranty defect in Product hardware reported to Carrier Access by BUYER during the warranty period, Carrier Access, as its sole obligation and BUYER's exclusive remedy for any breach of warranty, will use commercially reasonable efforts, at its option, to:

a. repair, replace, or service at its factory or on the BUYER's premises the Product, or component therein, or workmanship found to be defective so that the Product hardware operates substantially in accordance with Carrier Access Documentation, or

b. credit BUYER for the Product in accordance with Carrier Access's depreciation policy.

With respect to a warranty defect in the Licensed Software reported to Carrier Access by BUYER during the 90-day software warranty period, Carrier Access, at its own expense and as its sole obligation and BUYER's exclusive remedy for any breach of the software warranty, will use commercially reasonable efforts to, at its option,

a. correct any reproducible error in the Licensed Software, or

b. replace the defective Licensed Software, as follows:
Should a Severity 1 or 2 warranty defect with the Software occur during the 90-day warranty period, Carrier Access will provide, in its sole determination, either

1. software to resolve the defect to be downloaded into the affected units by the BUYER, or

2. a documented workaround to address the issue.

Severity 1 issues are failures of the Licensed Software to comply with the Carrier Access software specifications and that completely or severely affect the Carrier Access Product and its traffic or service capacity, or maintenance or monitoring capabilities.

Severity 2 issues are failures of the Licensed Software to comply with the Carrier Access software specifications and that result in a major degradation of the Carrier Access Product so as to impact its system or service performance, or significant impairments to network operator control or effectiveness. Should a Severity 3 warranty defect with the Licensed Software occur during the 90-day warranty period, Carrier Access will provide assistance to Buyer to determine if a solution or workaround will be provided in a subsequent software release following the reported issue.

Severity 3 issues are defined as failures of the Licensed Software to comply with the Carrier Access software specifications but that do not significantly impair the function or service of the Carrier Access Product or the system.

Determination of Severity 1, 2 or 3 shall be made solely by Carrier Access following receipt of the reported problem. Refurbished material may be used to repair or replace the Product. BUYER shall bear the risk of loss for Products or Software returned to Carrier Access for repair, replacement, or service, and the same must be shipped pre-paid by BUYER.

Requests for warranty services and troubleshooting must be made to, and will be provided by, the Carrier Access Customer Support Center via telephone during the warranty period and during normal business hours. Normal business hours for Carrier Access Customer Support Center are 7:00 a.m. to 6:00 p.m. Mountain Standard Time, Monday through Friday, excluding weekends and standard Carrier Access recognized holidays.

Limitation of Warranty & Limitation of Remedies

Correction of defects by repair, replacement, or service will be at Carrier Access's option and constitute Carrier Access' sole obligation and BUYER's sole and exclusive remedy under the limited warranty. Any such error correction or replacement provided to BUYER does not extend the original warranty period for hardware or software, respectively.

Carrier Access assumes no warranty or other liability with respect to defects in the Product or Software caused by:

a. modification, repair, storage, installation, operation, or maintenance of the Product or Software by anyone other than Carrier Access or its agent, or as authorized and in accordance with the Carrier Access Documentation, or

b. the negligent, unlawful or other improper use or storage of the Product or Software, including its use with incompatible equipment or software; or

c. fire, explosion, power failures, acts of God, or any other cause beyond Carrier Access' reasonable control, or

d. handling or transportation after title of the Product passes to BUYER.

Other manufacturer's equipment or software purchased by Carrier Access and resold to BUYER will be limited to that manufacturer's warranty. Carrier Access assumes no warranty liability for other manufacturer's equipment or software furnished by BUYER.

BUYER UNDERSTANDS AND AGREES AS FOLLOWS: Except for the limited warranty set forth above, the Product, License Software and all services performed by Carrier Access hereunder are provided “as is”, without representations or warranties of any kind. Carrier Access does not warrant that the Product, License Software, any hardware or software, or any update, upgrade, fix or workaround furnished to BUYER will meet BUYER's requirements, that the operation thereof, including any maintenance or major releases thereto will be uninterrupted or error-free.

THE WARRANTIES IN THIS AGREEMENT REPLACE ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, AND ALL OTHER OBLIGATIONS OR LIABILITIES OF CARRIER ACCESS, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT AND/OR ANY IMPLIED WARRANTIES ARISING OUT OF COURSE OF PERFORMANCE OR COURSE OF DEALING. ALL OTHER WARRANTIES ARE DISCLAIMED AND EXCLUDED BY CARRIER ACCESS.

THE REMEDIES CONTAINED IN THIS AGREEMENT WILL BE THE SOLE AND EXCLUSIVE REMEDIES WHETHER IN CONTRACT, TORT, OR OTHERWISE, AND CARRIER ACCESS WILL NOT BE LIABLE FOR INJURIES OR DAMAGES TO PERSONS OR PROPERTY RESULTING FROM ANY CAUSE WHATSOEVER, WITH THE EXCEPTION OF INJURIES OR DAMAGES CAUSED BY THE GROSS NEGLIGENCE OF CARRIER ACCESS. THIS LIMITATION APPLIES TO ALL SERVICES, SOFTWARE, AND PRODUCTS DURING AND AFTER THE WARRANTY PERIOD. IN NO EVENT WILL CARRIER ACCESS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, LOSS OF DATA, OR COMMERCIAL LOSSES EVEN IF CARRIER ACCESS HAS BEEN ADVISED THEREOF.

No agent, BUYER, or representative is authorized to make any warranties on behalf of Carrier Access or to assume for Carrier Access any other liability in connection with any of Carrier Access's Products, software, or services.

The foregoing summarizes Carrier Access' entire product and software warranties, which are subject to change without notice.

Warranty Product Returns

Before returning any equipment to Carrier Access Corporation, first contact the distributor or dealer from which you purchased the product.

A Return Material Authorization (RMA) number is required for all equipment returned to Carrier Access Corporation. Call Carrier Access Corporation Customer Support at (800) 786-9929 or (303) 442-5455 for RMA number, repair/warranty information and shipping instructions. Be prepared to provide the following information:

- Carrier Access Corporation serial number(s) from the system chassis or circuit card(s)
- Name of distributor or dealer from which you purchased the product
- Description of defect

TABLE OF CONTENTS

Preface

Compliance iii
Safety of Information Technology Equipment iii
FCC Requirements, Part 15 iii
FCC Requirements, Part 68 iii
Industry Canada ICES-003 v
Industry Canada CS-03 v
Safety Information vi
Notices vi
Electrostatic Discharge (ESD) Precautions vii
Warranty viii
Warranty Procedure viii
Limitation of Warranty & Limitation of Remedies ix
Warranty Product Returns x

1 Adit 3200 Base Platform

Overview 1-2
Speed Without Sacrificing Security and Performance 1-2
Simplified Configuration and Management 1-2
Key Benefits 1-2
Technical Specifications 1-3
Components 1-3
Interfaces 1-3
Network Standards 1-3
Routing and Policy Management 1-3
VPN 1-4
Router Performance 1-4
Quality of Service 1-4
Firewall Features 1-4
Management 1-4
Power 1-4
Regulatory Approvals 1-5
Physical Information 1-5
Environment 1-5
Chassis 1-6

2 Physical Installation

Unpacking and Inspection 2-2
Installation Environment 2-2
User Safety 2-3

Compliant Installation 2-3
Wall Mounting 2-5
Rack Mounting 2-6
Adit 3104, 3200, 3300 and 3400 Battery Backup 2-8

3 Electrical Installation & Cabling

Adit 3200 3-2
Connections 3-2
Interface Connectors 3-3
Grounding the Unit 3-3
Power 3-4
Battery Connection 3-4
RS-232 Craft Port (Female DB-9) 3-5
DS1/E1 Connection Ports 3-6
10/100Base-TX Ethernet 3-7
Reset Button 3-8
Alarm/Status LEDs 3-8

4 Configuration

PC Network Configuration 4-2
LAN Connection 4-3
Internet Connection 4-3
Web-Based Management 4-4
To access the management console 4-4
Setting up a CLI Connection 4-5
Log in 4-6
Key Enabled Software Features 4-7
Basic Configuration 4-8
Setup Adit 3200 for access via Web-Browser 4-8
Restore Factory Defaults 4-9
Modify Default Admin User 4-10
Configure Ethernet WAN Interface 4-12
Configure Serial 1 as WAN 4-14

Glossary

Index

CHAPTER 1

Adit 3200 Base Platform

In this Chapter

- Overview
- Technical Specifications
- Chassis

Overview

The Adit 3200 series IP Business Router is a new breed of access equipment designed to deliver hosted voice and data services at a disruptive price with unmatched performance, engineered to withstand the inherent stress of an enterprise environment. The Adit 3200 integrates the features of a high-performance router and a stateful firewall with flexile WAN interface options. It replaces multiple elements at the customer premise offering a powerful blend of speed, security, data, hosted VoIP and integrated applications on a single reliable platform. Companies can realize significant cost reduction by taking advantage of a single managed entity to deliver high-value services and availability to their business and enterprise customers.

The integrated design provides the ability to upgrade bandwidth (T1 to Ethernet) and capabilities without the need to replace hardware platforms. Additionally, the Adit 3200 provides integral support for important applications such as VPN, VoIP ALG and DMZ.

Speed Without Sacrificing Security and Performance

The Adit 3200 includes a complete stateful and transparent firewall that inspects, blocks, filters or translates every packet. Stateful firewall functions are combined with application and IP traffic aware protection. Unlike competing offerings, the Adit 3200 maintains wire-speed throughput with low latency for all packet sizes with security features, such as multiple firewall rules and VPN tunnels, turned on. The Adit 3200's VoIP-aware routing engine is based on the latest advanced network processing technology and enables support of key security applications without the typical degradation in performance seen in other legacy solutions on the market.

By integrating all routing and security functions into a single processor, the Adit 3200 cost-effectively supports VPN tunnels, Network Address Translation (NAT/NAPT), stateful packet inspection, flow classification, SIP ALG and intrusion detection. Access control lists also protect traffic flowing in and out of the network. Integrated firewall keeps the network segments secure from intrusions and attacks while allowing authorized access to network resources. VPN provides secure IP access to customers with support for DES, 3DES and AES encryption. All these features are provided in a single reliable platform achieving 99.998% uptime thanks to the lack of any moving parts and excellent heat dissipation.

Simplified Configuration and Management

The Adit 3200's scalability does not increase its complexity. It enables the unified management of what were multiple platforms in the network. Remote provisioning is simplified through both an easy-to-use web nterface and an intuitive command line interface. Remote alarms from the Adit 3200 are reported via SNMP, Syslog, e-mail alerts, or through a web interface. The router can also be automatically configured and upgraded remotely.

Key Benefits

- Comprehensive router, flexible WAN connection, firewall and managed Ethernet switch in a single platform with price-disruptive features and performance
- Speed without sacrificing security to deliver public and private IP access at wire-speed across all packet sizes
- Web-enabled stateful firewall provides integrated network-level and application-level protection
- Scalable application that provides data with QoS required for carrier-grade VoIP
- Carrier grade reliability, performance and life cycle to enable mission critical business applications

Technical Specifications

Components

- Included Accessories
  - Wall mount bracket
- Additional Accessories
  - Adit 3000 Battery Backup Unit
  - Adit 3000 Rack Mount Kit

Interfaces

- T1 WAN port (RJ-48C connector)
  - Framing for T1: SF (D4) or ESF
  - Line Code for T1: B8ZS or AMI
  - Internal or line-derived clock source
  - T1 Loop Codes and BERT testing
- 10/100Base-T WAN port (RJ-45 connector)
- 4 10/100Base-T switched LAN ports (RJ-45 connector)
- RS-232 for local management (DB-9 connector)

Network Standards

- ANSI/TIA T1.231, T1.403, T1.413 i2
- ITU G.703, G.704

Routing and Policy Management

- IPv4
- Static routes
- RIP v1, v2
- OSPF
- PPP
  - ACF, VJ compression
- Spanning Tree Protocol (802.1d)
- DHCP Server/Client/Relay
- DNS Relay and Resolver
- BootP Relay
- PAP and CHAP authentication
- Ping
- IPCP, BCP
- Multi-Protocol Encapsulation
- VLAN support

VPN

- IPSec tunneling and PPTP & L2TP support
- DES, 3DES and AES
- IKE-based key management
- Digital certificates and pre-shared key authentication

Router Performance

- Wire-speed on Ethernet to T1 interface

Quality of Service

- ToS marking and interpretation per IETF Std. 5
- VLAN Priority Queuing

Firewall Features

- Stateful Firewall
- NAT/NAPT, NAT Bypass, NAT Pin-Holes
- L1-L4 Flow Classification
- Application Layer Gateway
- Denial of Service Filtering
- Intrusion Detection

Management

- Status indicators
- SNMP v1, v2c (10/100Base-T or in-band network)
- Standard MIBs
- Command Line Interface (CLI), FTP, telnet, TFTP
- CLI over secure telnet
- Web-based interface over SSL
- RADIUS
- Syslog

Power

- AC Input Voltage: 120/240 VAC @ 60/50 Hz
- DC Input Voltage -48 VDC, 1 amp
- Internal solid-state (fuseless) protection

Regulatory Approvals

USA

- UL60950
- FCC Part 15, Class A
- FCC Part 68

Canada

- CSA 60950-1
- ICES-003, Class A
- CS-03

Physical Information

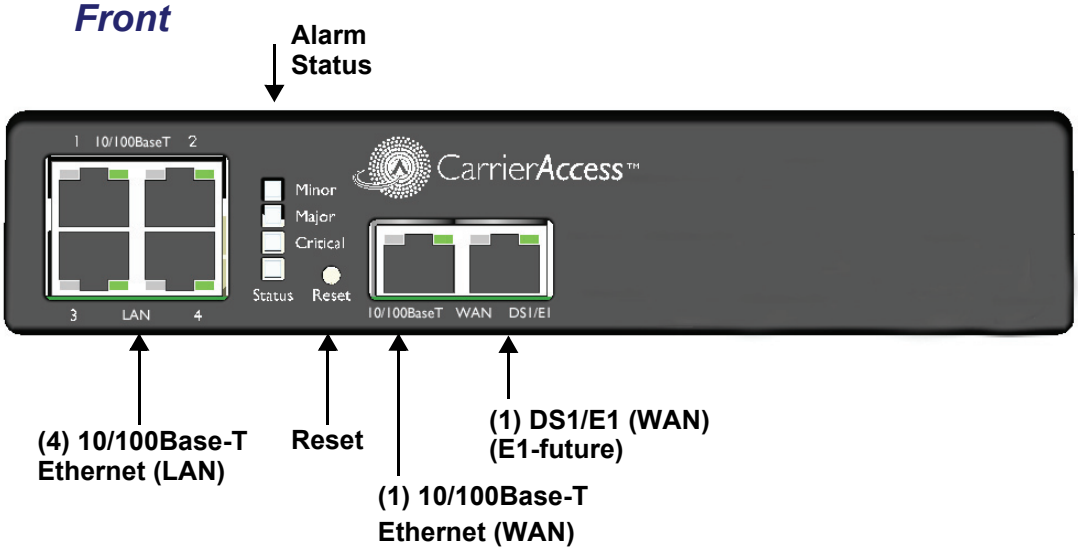
- Wall mount brackets (included)
- Rack mount options: 19 or 23 inch rack
- Dimensions: 1.75 in. (H-2 RU) x 8.25 in. (W) x 12 in. (D)
  4.4 cm (H) x 21 cm (W) x 30.5 cm (D)
- Weight: 6.25 lbs. (2.83 kg)

Environment

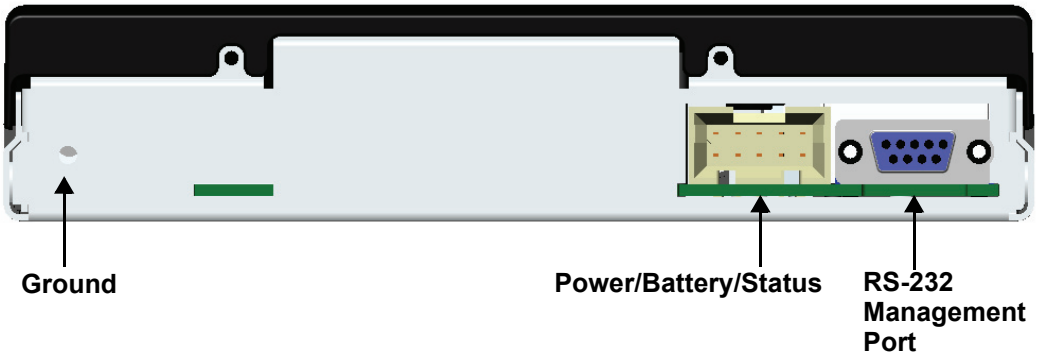
- Operating temperature range: 32 °F to 104 °F (0 °C to 40 °C)
- Storage temperature range: -40 °F to 158 °F (-40 °C to 70 °C)
- Maximum operating altitude: 10,000 ft. (3,048 m)
- Maximum non-operating altitude: 40,000 ft. (12,192 m)
- Relative humidity (non-condensing) range: 0% to 95%

Chassis

Front



Back



CHAPTER 2

Physical Installation

In this Chapter

- Unpacking and Inspection
- Installation Environment
- Compliant Installation
- Wall Mounting
- Rack Mounting
- Adit 3104, 3200, 3300 and 3400 Battery Backup

Unpacking and Inspection

WARNING! **OBSERVE PRECAUTIONS FOR HANDLING ELECTROSTATIC DEVICES.**

1. Inspect containers for damage during shipment. Report any damage to the freight carrier for possible insurance claims.
2. Compare packing list with office records. Report any discrepancies to the office.
3. Open shipping containers, be careful not to damage contents.
4. Inspect contents and report any damage.
5. If equipment must be returned for any reason, carefully repack equipment in the original shipping container with original packing materials if possible.
6. If equipment is to be installed later, replace equipment in original shipping container and store in a safe place until ready to install.

Installation Environment

The environment in which you are installing the Adit 3000 must meet the following conditions:

- Operating temperature range: 32° to 104° F (0° to 40° C)
- Storage temperature range: -40° to 158° F (-40° to 70° C)
- Maximum operating altitude: 10,000 ft. (3,048 m)
- Maximum non-operating altitude: 40,000 ft. (12,192 m)
- Relative humidity (non-condensing) range: 0 to 95%

WARNING! **THE ADIT 3000 IS DESIGNED FOR WALL AND RACK MOUNTING ONLY. IT IS NOT DESIGNED FOR DESKTOP USE.**

User Safety

CAUTION! WHEN USING YOUR TELEPHONE EQUIPMENT, BASIC SAFETY PRECAUTIONS SHOULD ALWAYS BE FOLLOWED TO REDUCE THE RISK OF FIRE, ELECTRIC SHOCK AND INJURY TO PERSONS, INCLUDING THE FOLLOWING:

- Do not use this product near water for example, near a bathtub, washbowl, kitchen sink or laundry tub, in a wet basement or near a swimming pool.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- Do not use the telephone to report a gas leak in the vicinity of the leak.
- Use only the power cord and batteries indicated in this manual. Do not dispose of batteries in a fire. They may explode. Check with local codes for possible special disposal instructions.
- Refer to the installation section of this manual for a safe and proper installation procedure. All wiring external to this equipment should follow the current provision of the National Electrical Code

Compliant Installation

The following are instructions for a compliant installation of the Adit 3200. Please note the following warnings, before installing the unit.

For wall and rack mount instructions, use the links listed below to the appropriate section:

- Wall Mounting
- Rack Mounting

WARNING! OBSERVE PRECAUTIONS FOR HANDLING ELECTROSTATIC DEVICES. SEE PREFACE, ELECTROSTATIC DISCHARGE (ESD) PRECAUTIONS FOR DETAILED INFORMATION.

WARNING! THE T1 NETWORK INTERFACES ARE CERTIFIED WITH THE FCC AND INDUSTRY CANADA FOR DIRECT CONNECTION TO PUBLIC COMMUNICATION NETWORKS. SECONDARY LIGHTNING SURGE AND AC POWER CROSS PROTECTION IS PROVIDED. UTILIZE LISTED PRIMARY PROTECTORS WITH A NOMINAL 230V BREAKDOWN RATING TO ENSURE VOLTAGE COORDINATION WITH SECONDARY PROTECTION. THE INSTALLER IS REQUIRED TO FOLLOW LOCAL OR NATIONAL ELECTRIC CODES FOR COMMUNICATION CIRCUITS.

NOTE: It is important the DS1/E1 Network Interface Cables are secured separately from the power and Signal Cables.

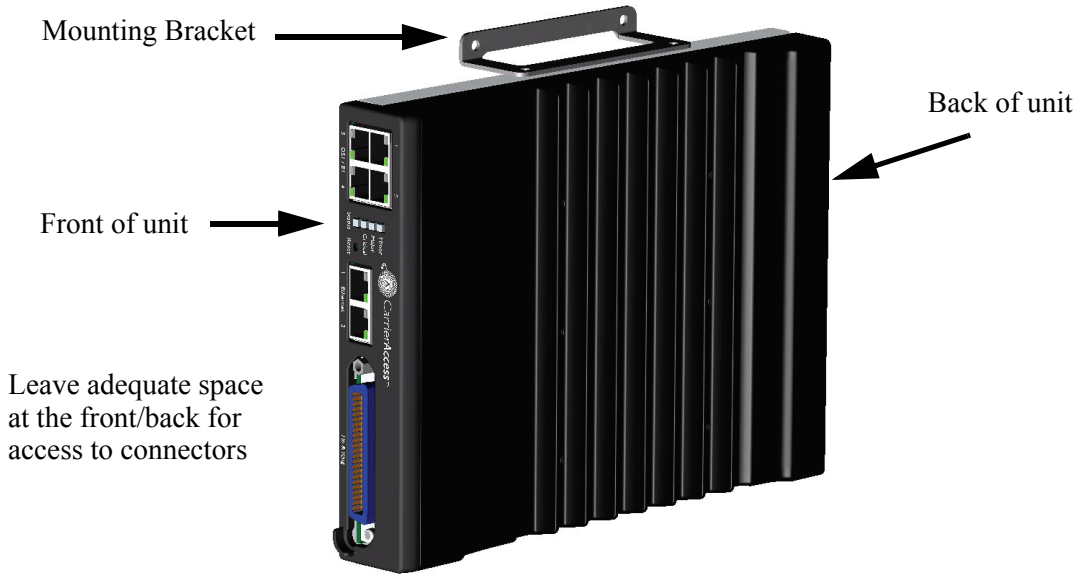
1. Inspect the unit.
2. Mount the unit, see *Wall Mounting* on page 2-5, or *Rack Mounting* on page 2-6 for detailed instructions.
3. Ground the unit.

WARNING! THE SEPARATE PROTECTIVE EARTHING TERMINAL PROVIDED ON THIS PRODUCT SHALL BE PERMANENTLY CONNECTED TO EARTH. SEE *GROUNDING THE UNIT* ON PAGE 3-3.

4. Connect DS1 (T1) and Ethernet connectors as needed.
5. Connect RS-232 connector and open Terminal Emulator software on your PC. Note: With this connected first, the boot process can be monitored.
6. Connect Power to the unit.
7. Monitor the boot process on your PC, when complete the status light should be green.
8. For any software enabled features, enter the key command. See the **key** command in the Adit 3000 CLI Reference Manual, for detailed information.
9. To verify use the **show version** command.
10. Now you can proceed to provisioning the unit. See *Chapter 4, Configuration* for information.

Wall Mounting

Before beginning the mounting process, verify that the installation area is a stable environment, clean and free from extremes of temperature, shock, vibration and EMI. See *Installation Environment* on page 2-2.



The Adit 3000 is delivered with mounting brackets that can easily be attached for quick and easy wall mounting, as shown in the illustration above.

To install the unit to the wall:

1. Attach the wall mount brackets to the Adit 3000, with wall attachment flange pointing away from the unit, as shown above. Attach with 4 screws provided (2 for each bracket).
2. Mount the unit to the wall using appropriate mounting screws (not included). Note: It is acceptable to mount on drywall with suitable anchor-type mounting screws.

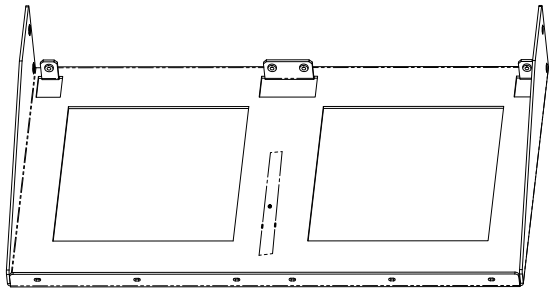
NOTE: The Adit 3000 must be mounted with the brackets on the top and bottom, as shown above.

Rack Mounting

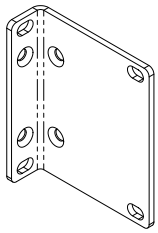
NOTE: Rack mounting kits are available for both 19 and 23 inch racks. 1 Rack Unit (RU) of spacing is required above the Adit 3000 in the Rack Mount Unit.

To rack mount the Adit 3000, follow the instructions below:

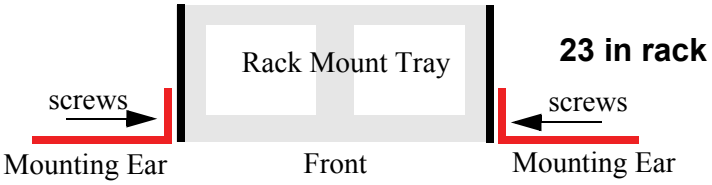
1. Attach bracket ears to Rack Mounting Tray using four #10-32 x 1/4" screws on each side. The Mounting Ears can be used for both a 19 or 23 inch rack. The drawing below shows a top view of the 2 versions.

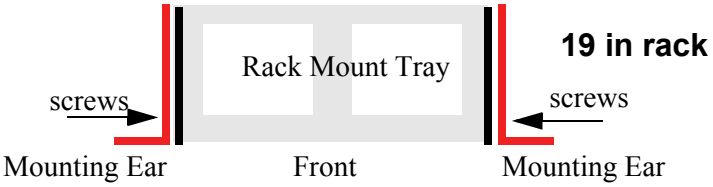


Rack Mounting Tray



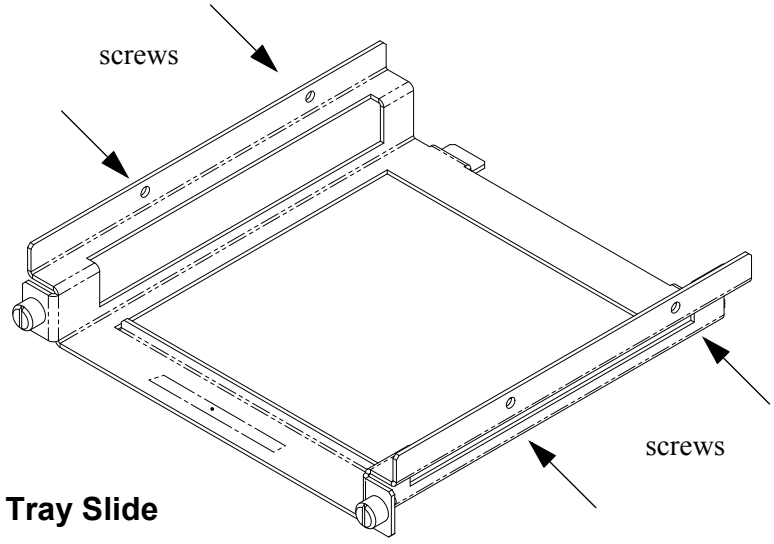
Mounting Ear



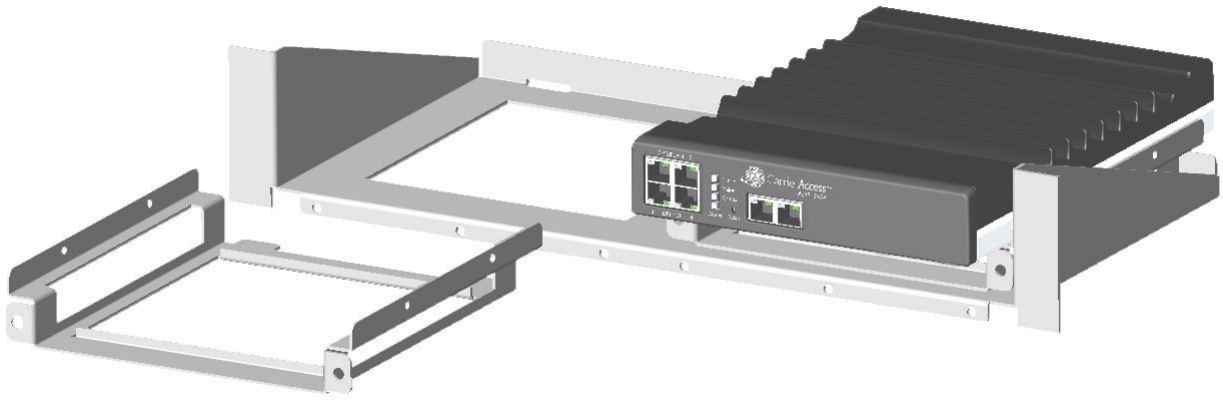


2. Attach the Rack Mounting Tray assembly (with mounting ears attached) to rack, using four #10-32 x 1/4" screws (two on each mounting ear).
3. Remove wall mount and screws, if attached, from Adit 3000 unit.
   Note: Adit 3000 and wall mounting bracket are not assembled from the factory.

4. Place the Adit on the Tray Slide and attach with 4 screws removed in step 2.



5. Slide the assembled piece (Adit 3000 and Tray Slide) onto the installed Rack Mounting Tray.



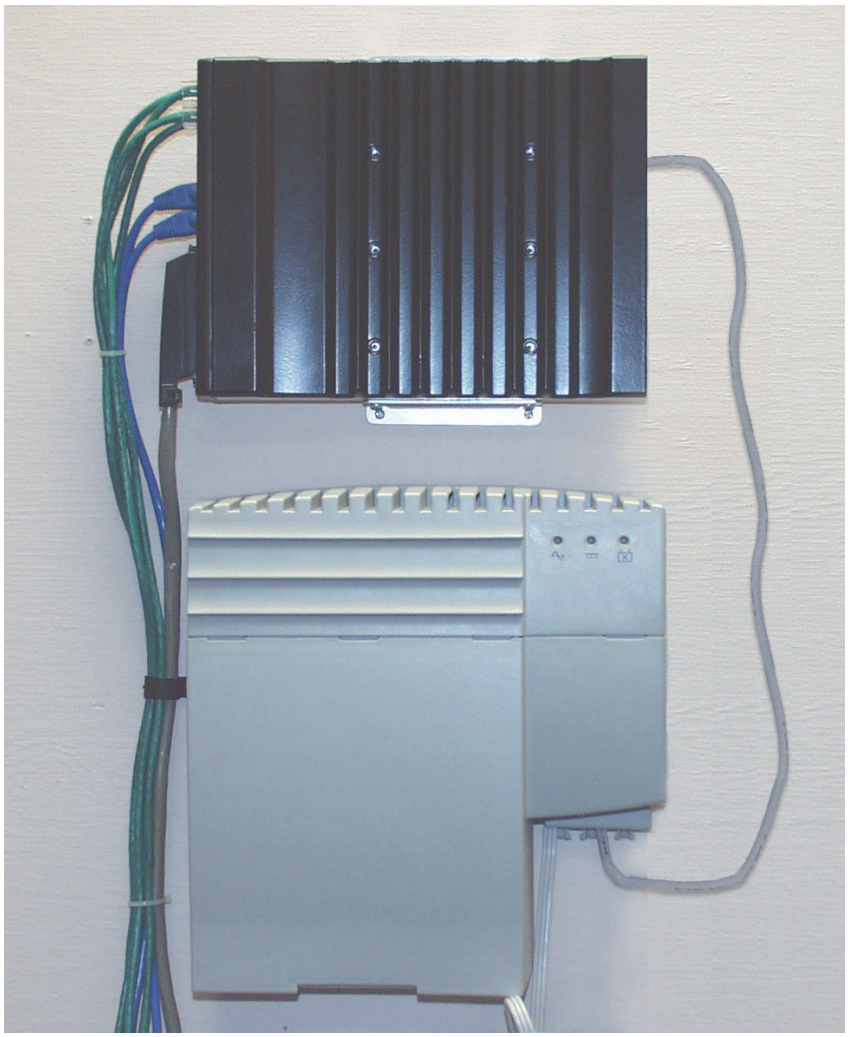
6. Secure the Tray Slide to the Rack Mounting Tray with the attached screws on the Tray Slide.

Adit 3104, 3200, 3300 and 3400 Battery Backup

The Adit 3104, 3200, 3300 and 3400 Battery Backup (P/N 730-0132), is a wall-mount battery backup unit to provide up to 8 hours battery backup.

Please see the Battery Backup User Manual for product information and installation instructions, which is provided with unit.

Note: This is an optional feature.



CHAPTER 3

Electrical Installation & Cabling

In this Chapter

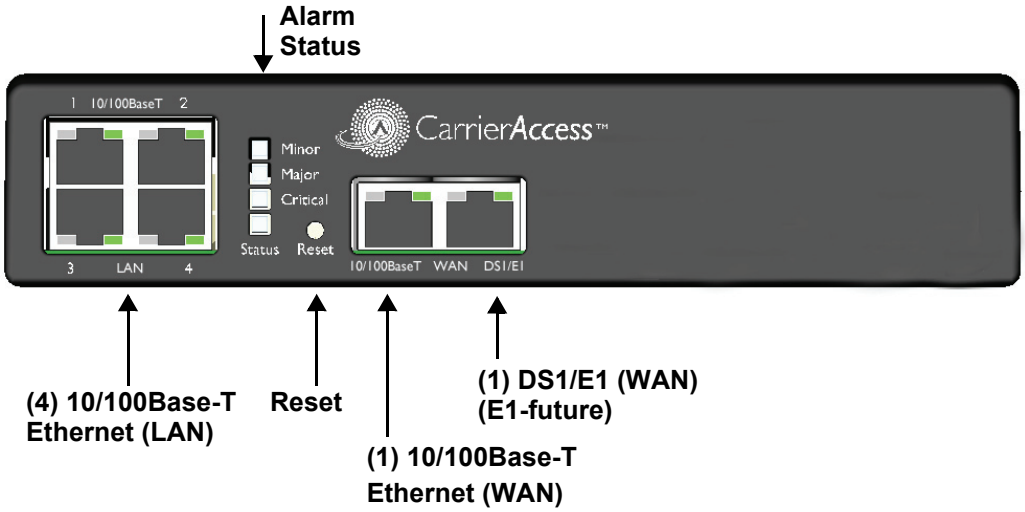
- Adit 3200
- Interface Connectors
- Reset Button
- Alarm/Status LEDs

Adit 3200

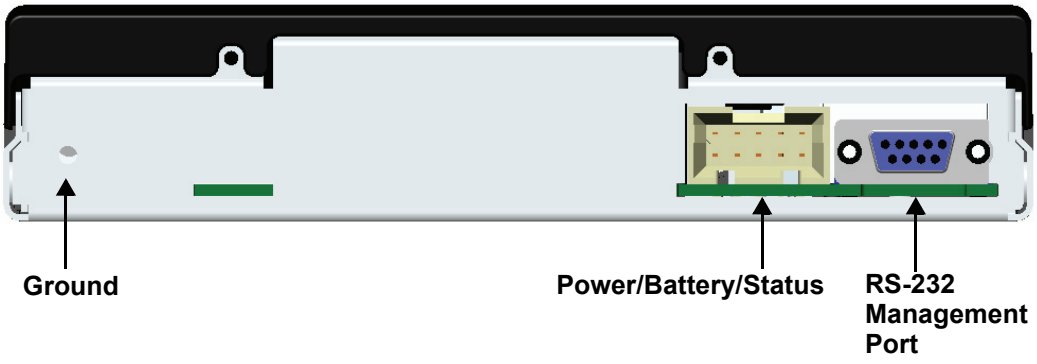
Connections

The following illustrations show all connectors on the Adit 3200.

Front



Back



Interface Connectors

The following are the Adit 3200 interface connectors:

Front of Adit

- (1) DS1 WAN port (RJ-48C). Note: E1 will be in a future release.
- (1) 10/100Base-T WAN port (RJ-45)
- (4) 10/100Base-T switched LAN ports (RJ-45)

Back of Adit

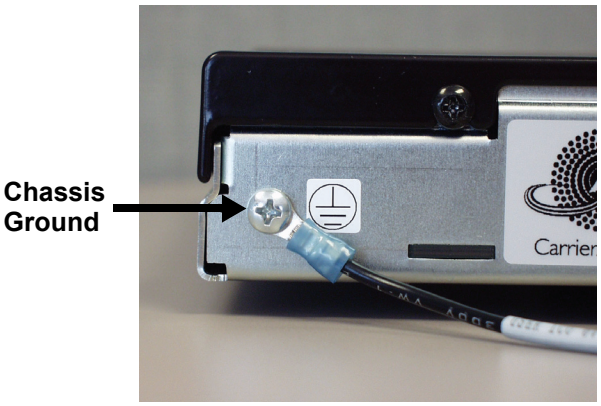
- RS-232 craft port connector for local management
- Power input connector
- Ground connector

Grounding the Unit

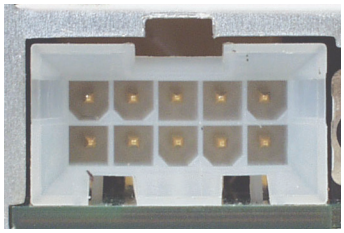
WARNING! THE ADIT 3200 ARE REQUIRED TO BE PERMANENTLY GROUNDED FOR THE PROTECTION OF USERS AND SERVICE PERSONNEL.

Chassis ground is located on the back of the unit. To ground the unit:

1. Connect a minimum 14 AWG ground wire with a #8 ring tongue terminal (not included) to the chassis ground on the back of the unit. Secure with the 8-32 screw and lock washer provided.
2. Connect the opposite end of the ground wire to a suitable earth grounding point such as a building grounding electrode, metal water pipe, or metal building structure that is in compliance with article 250 of NEC.



Power



The Adit 3000 is powered by a limited -48 VDC Power source. The following options are available:

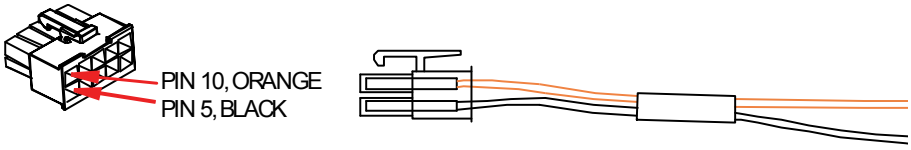
- AC/DC Converter
- Battery Backup module

AC/DC Converter

An AC/DC Converter generates 48VDC from any worldwide AC power source.

To connect AC power:

1. Plug power connector from AC/DC converter into rear of Adit 3000.
2. Connect AC/DC converter to wall outlet.
3. A green light should appear on the Status LED on the front of the unit.



CAUTION! **INCORRECT WIRING OF CORD MAY CAUSE EXTERNAL FUSE FAILURE.**

WARNING! **POSSIBLE SHOCK HAZARD EXISTS, PLEASE FOLLOW INSTRUCTIONS CAREFULLY.**

To connect -48 VDC power:

1. Wire appropriate connector to open end of the DC Power cable.
   Orange = -48 Black = Ground (+)
2. Plug the DC power connector in the -48 VDC input power connector.
3. Apply power to connector from -48 VDC power source.
4. A green light should appear on the Status LED on the front of the unit.

WARNING! **EXTERNAL FUSE PROTECTION IS REQUIRED ON THE 48VDC INPUT WHEN CONNECTED TO A DC POWER SOURCE NOT SUPPLIED BY CARRIER ACCESS.**

Fuse Recommendations, or equivalent:

Recommended Fuse	AMP Rating
Littelfuse 48101.5	1.5 Amp
Bussman GMC-1.5A	1.5 Amp

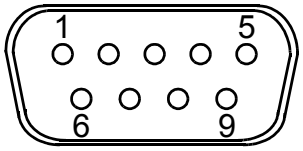
Battery Connection

The Adit 3000 Battery connection is provided for Battery Backup. See *Adit 3104, 3200, 3300 and 3400 Battery Backup on page 2-8* for additional information.

RS-232 Craft Port (Female DB-9)

The RS-232 craft port connector (female) is for connection to an external PC or Hayes-compatible modem for local or remote configuration, management, and performance monitoring using the Adit 3000 Command Line Interface (CLI).

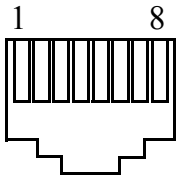
The RS-232 craft port connects via a female DB-9 connector on the Adit 3000.



The pinouts are as follows:

Pin Number	Direction	Description
1	Outbound	Carrier Detect
2	Outbound	Receive Data
3	Inbound	Transmit Data
4	Inbound	Data Terminal Ready
5	N/A	Signal Ground
6	Outbound	Data Set Ready
7	Inbound	Request to Send
8	Outbound	Clear to Send
9	N/C	Not connected

DS1/E1 Connection Ports



Each DS1/E1 connection port is equipped with a standard RJ-48C (female) on the Adit 3000 unit. Note: E1 will be available in a future release.

The pinouts are as follows:

DS1/E1 RJ-48C

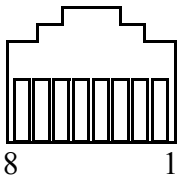
The pinouts are as follows:

Pin	Name	Description
1	Receive Ring	Receive from DS1 network
2	Receive Tip	Receive from DS1 network
3	N/C	Not connected
4	Transmit Ring	To DS1 network
5	Transmit Tip	To DS1 network
6-8	N/C	Not connected

The LEDs are as follows (left LED only):

State	Description
Off	Off line
Green	Normal
Red	Loss of Signal (LOS)
Yellow	Bipolar Violation (BPV)
Flashing Green	Loopback active
Flashing Yellow	Yellow Alarm (Remote Alarm Indication)
Flashing Red (Slow)	Loss of Frame (LOF) or Alarm Indication Signal (AIS)
Flashing Red (Fast)	Self-test Failure

10/100Base-TX Ethernet



The 10/100Base-TX Ethernet (female) ports provide connectivity for Router WAN and/or LAN ports and for management connection via Telnet and/or SNMP to a Network Management System.

Ethernet (RJ-45)

The pinouts are as follows:

Note: This is a hub pinout, you will need a straight cable to connect to a PC.

Pin	Name	Description
1	Receive +	Receive from network
2	Receive -	Receive from network
3	Transmit +	Transmit to network
4-5	N/C	Not connected
6	Transmit -	Transmit to network
7-8	N/C	Not connected

The LEDs are as follows:

LED	State	Description
Left LED	The left LED shall show Link Status.	
	Off	Link Down
	Green	Link Up
	Flashing Green	Traffic on Link
	Yellow	Collision status
Right LED	The right LED shall indicate Link Speed.	
	Off	10 Mbit/sec, down or not connected
	Green	100 Mbit/sec

Reset Button

The system can be reset by pressing the reset button located on the front panel.

Alarm/Status LEDs

LED	State	Description
Critical	Off	No critical alarms present
	Red	Critical alarms present. Critical alarms include: user-configured manor environmental inputs.
Major	Off	No major alarms present
	Red	Major alarm present. Major alarms include: user-configured manor environmental inputs, DS1 short, DS1 open, DS1 facility alarm, DS1 RAI, DS1 AIS, DS1 LOF, DS1 LOS, WAN fault, Ethernet fault and dead card alarms.
Minor	Off	No minor alarms present
	Red	Minor alarms present. Minor alarms include: user-configured minor environmental inputs, DS1 excessive line code violations.
Status	Off	No power to system
	Green	Application running, no detected system problems.
	Green Flashing	Power-On Self Test (POST) successful. System booted. Loading Application.
	Green/Yellow	Flashing alternate colors. Application Self Test in Process.
	Yellow	Yellow while booting. If this stays a steady yellow the Power-On Self Test (POST) failed.
	Yellow Flashing	Power-On Self Test (POST) In Process.
	Red	System Failure

CHAPTER 4

Configuration

After the Adit 3200 is installed (see *Compliant Installation on page 2-3)*, the system can now be provisioned.

In this Chapter

- PC Network Configuration
- Web-Based Management
- Setting up a CLI Connection
- Log in
- Key Enabled Software Features
- Basic Configuration
  - Setup Adit 3200 for access via Web-Browser
  - Restore Factory Defaults
  - Modify Default Admin User
  - Configure Ethernet WAN Interface
  - Configure Serial 1 as WAN

PC Network Configuration

When a PC is connected directly or indirectly to the Adit 3200 Ethernet LAN port (Eth-1), IP addresses will be acquired using the DHCP server or relay functionality of the Adit 3200.

Note: For either of these cases, the PC must be configured as a DHCP Client.

This configuration principle is identical but performed differently on each OS.

Windows XP

1. Access **Network Connections** from the Control Panel.
2. Right-click the Ethernet connection's icon, and select **Properties** to display the connection's properties.
3. From the **General** tab select the **Internet Protocol (TCP/IP)** component and press the **Properties** button.
4. The Internet Protocol (TCP/IP) properties will be displayed and the following must be selected.
   - Select the **Obtain an IP address automatically.**
   - Select the **Obtain DNS server address automatically**.
5. Continue on the following setup for a LAN Connection.

Windows 2000/98/Me

1. Access **Network and Dialing Connections** from the Control Panel.
2. Right-click the Ethernet connection's icon, and select **Properties** to display the connection's properties.
3. Select the **Internet Protocol (TCP/IP)** component and press the **Properties** button.
4. The Internet Protocol (TCP/IP) properties will be displayed and the following must be selected.
   - Select the **Obtain an IP address automatically.**
   - Select the **Obtain DNS server address automatically**.
5. Continue on the following setup for a LAN Connection.

Windows NT

1. Access **Network** from the Control Panel to display the network control panel.
2. From the **Protocol tab** select the **Internet Protocol (TCP/IP)** component and press the **Properties** button.
3. From the **IP Address** tab select **Obtain an IP address automatically**.
4. From the **DNS Address** tab verify that no DNS server is defined in the **DNS Service Search Order** field**,** and no suffix is defined in the **Domain Suffix Search Order** field.
5. Reboot
6. Continue on the following setup for a LAN Connection.

Linux

1. Login into the system as a super-user, by entering **su** at the prompt.
2. Type **ifconfig** to display the network devices and allocated IP's.
3. Type **pump -i dev**, the dev is the network device name.
4. Type **ifconfig** again to view the new allocated IP address.
5. Continue on the following setup for a LAN Connection.

LAN Connection

Your computer can connect to the gateway in various forms, each requiring a different physical connection. See *Chapter 3, Electrical Installation & Cabling.*

Internet Connection

Connect the gateway directly to the Internet.

Web-Based Management

The web-based management interface allows you to control various system parameters. The interface is accessed through a web browser.

To access the management console

NOTE: The following assumes that you have connected the PC to the LAN port of the Adit 3200.

1. Launch a web browser on your PC in the LAN to which the Adit 3200's LAN port is connected. Note: If connection to the Adit 3200 is to be through an Ethernet or T1 WAN, the remote admin WAN access must be enabled with the following command sequence:

Command	Description
`Username: admin` `Password: ********`	Log into the system (username and password).
`Adit 3200> enable`	Enter the Privileged mode.
`Password: ********`	Enter password for the Privileged mode.
`#configure terminal`	Enter the Configuration mode.
`(config)# remote-admin web primary-port enable`	Enable remote web admin.

2. Type the Adit 3200's IP address or name in the address bar.
   Example: http://192.168.1.1.
   - Default IP address is **http://192.168.1.1**
     Note: To display the current IP address of the systems, use the following CLI command:
     #show interface ethernet 1 (LAN)
     #show interface ethernet 2 (Eth WAN)
3. Login to the unit.
   Enter User Name and Password. Note: These setting should be changed from the default settings after the initial login.
   - Default user name is **admin**
   - Default password is **admin 123**

NOTE: After a few minutes of inactivity, the session will automatically timeout and the operator will be required to log in to continue the session.

WARNING! IF YOUR USER NAME AND PASSWORD ARE SET TO THE DEFAULT SETTING, IT IS RECOMMENDED THAT YOU MODIFY THEM FOR SECURITY PURPOSES.

Setting up a CLI Connection

A CLI connection will require the LAN or WAN IP address of the unit. Note: If the WAN IP address is used, the remote admin WAN access must be enabled with the following command sequence:

Command	Description
`Username: admin` `Password: ********`	Log into the system (username and password).
`Adit 3200> enable`	Enter the Privileged mode.
`Password: ********`	Enter password for the Privileged mode.
`#configure terminal`	Enter the Configuration mode.
`(config)# remote-admin web primary-port enable`	Enable remote web admin.

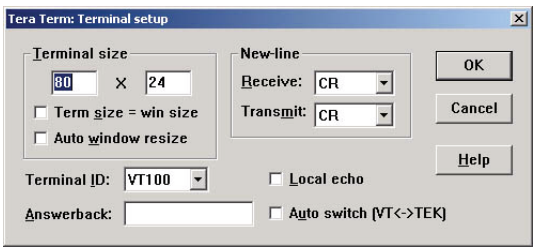
NOTE: For Adit 3200 CLI commands see the *Adit 3000 CLI Reference Manual.* This is a separate document and can be found on the CD that is provided with the product, or on the Carrier Access customer website.

To connect with CLI, set up the connection:

- If connecting via the Ethernet 100Base-T connection, use a Telnet TCP/IP program to access the CLI. This requires an IP address of the unit.
  Note: To display the current IP address of the unit, use the **ifconfig** command.
- If connecting via RS-232, the port settings should be set to:
  Bits per second: **115200** Data bits: **8**
  Parity: **None** Stop bits: **1**
  Flow control: **None**
- Set your Terminal Emulation to: **VT100**

NOTE: When using Tera Term (Telnet program) TCP/IP, CLI commands will not be recognized until the following setup is completed.

- In Tera Term go to **Setup/Terminal**
- Set the **New-line/Transmit** value **CR**



Log in

After successful connection, via telnet or HyperTerm, the user must login. Default Logins are:

Login: **admin**

Password: **admin123**

After successful login the prompt will be displayed as follows:

Adit 3200>

Note: It is recommended that you change your password from the default. See the following to modify the Admin level password on your system.

- GUI interface - see **Advanced/Users** window
- CLI interface - use the **Adit 3000(config)#username** command

Key Enabled Software Features

The Adit 3200 has additional features that are not provided on the base system. These features can be purchased with the product or added later as needed. These features are enabled via a Software Key (example: G.729). The number of keyed features may expand with the development of the product, therefore to see a list of current keyed features, or to purchase a key, contact Carrier Access Customer Service or Sales.

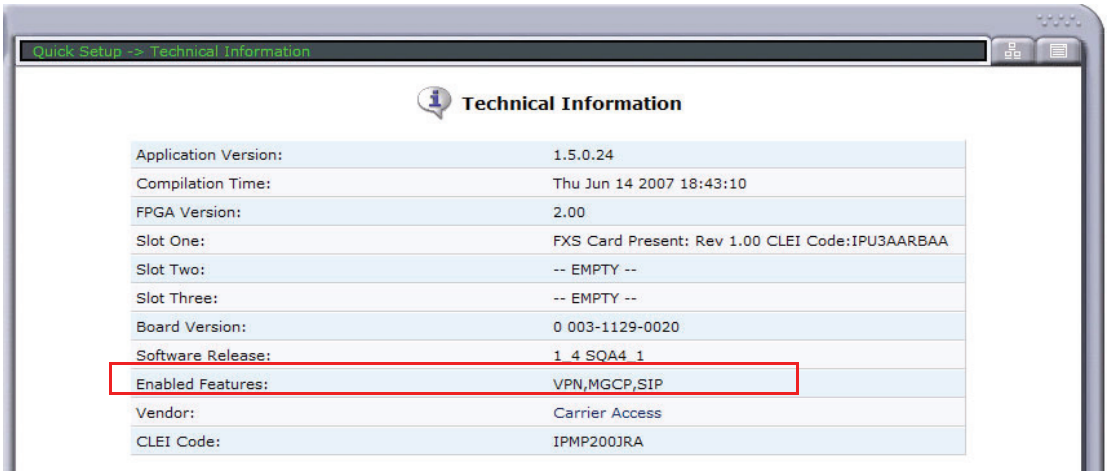
To enter a software key, use the following CLI command:

Syntax: **(config)# key {*key-code*}**

Example: **(config)# key cxusdfutkj3diosn412C**

NOTE: Keys may only be entered through the CLI (not through the GUI).

The Key Enabled Software Features are displayed on the **Advanced/Technical Information** window.


Quick Setup -> Technical Information
Technical Information
Application Version: 1.5.0.24
Compilation Time: Thu Jun 14 2007 18:43:10
FPGA Version: 2.00
Slot One: FXS Card Present: Rev 1.00 CLEI Code:IPU3AARBAA
Slot Two: -- EMPTY --
Slot Three: -- EMPTY --
Board Version: 0 003-1129-0020
Software Release: 1_4 SQA4_1
Enabled Features: VPN,MGCP,SIP
Vendor: Carrier Access
CLEI Code: IPMP200JRA

This information is also displayed with the following CLI command:

```
Adit 3200> show version
Application Version: 1.6
Compilation Time: Thu Jun 14 2007 18:43:10
FPGA Version: 2.00
Board Version: 0 003-1129-0020
IXP400 Software Release: 1_4 SQA4_1
Voice Slot 1 : FXS Card Present: Rev  1.00  CLEI Code:IPU3AARBAA
Voice Slot 2 : -- EMPTY --
Voice Slot 3 : -- EMPTY --
Vendor: Carrier Access
CLEI Code: IPMP200JRA
Product Features:
 VPN  enabled.
 MGCP enabled.
```

Basic Configuration

The following configuration is divided into logical sections, where each section configures an additional function. The first must be configured before the second and so forth, however, you may stop at any section and not add the following feature.

NOTE: The order in which commands are entered can affect the successful provisioning of the Adit 3200.

- **Setup Adit 3200 for access via Web-Browser**
- **Restore Factory Defaults**
- **Modify Default Admin User**
- **Configure Ethernet WAN Interface**
- **Configure Serial 1 as WAN**

Setup Adit 3200 for access via Web-Browser

The following steps will configure the Adit 3200 to allow access to the Web Browser for configuration, through one of the 4 10/100Base-T LAN connections.

Note: For LAN access, no additional configuration is required to access the Adit 3200 using the web browser.

To configure the WAN access:

1. Connect to the CLI via the DB-9 RS-232. See *Setting up a CLI Connection on page 4-5*.
2. Enable the remote admin WAN access with the following command sequence:

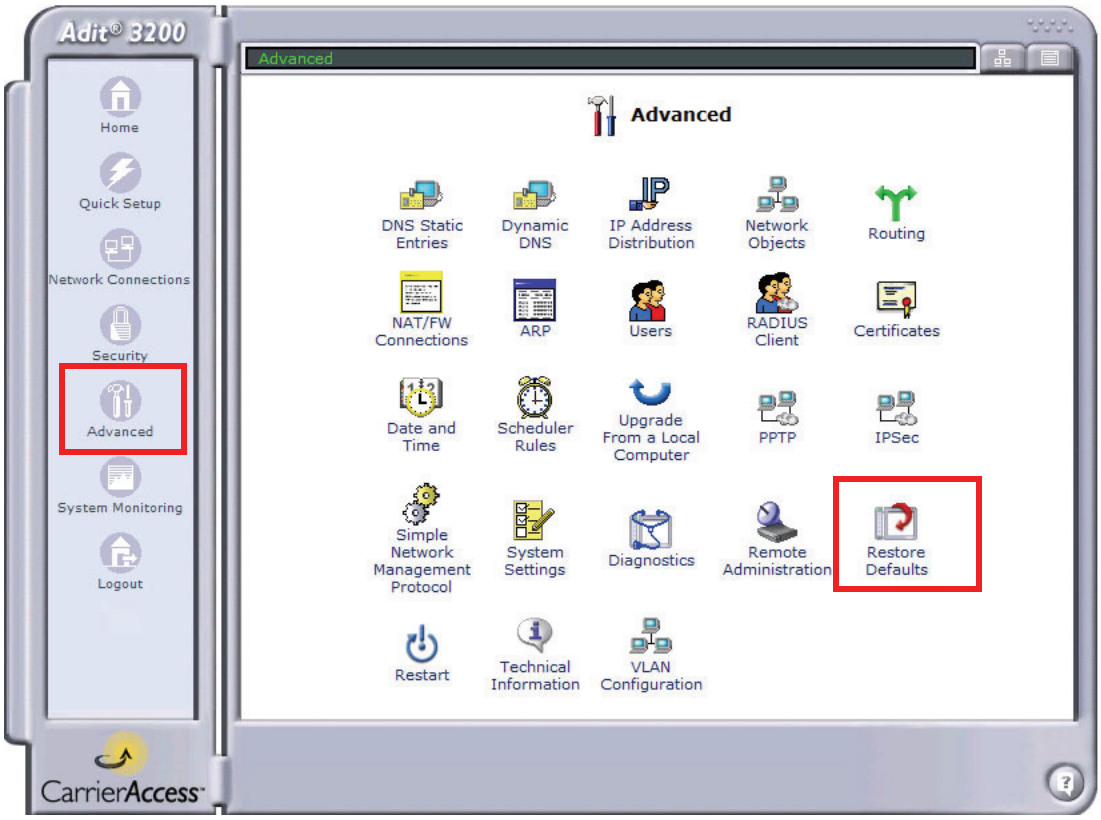
Command	Description
`Username: admin` `Password: ********`	Log into the system (username and password).
`Adit 3200> enable`	Enter the Privileged mode.
`Password: ********`	Enter password for the Privileged mode.
`#configure terminal`	Enter the Configuration mode.
`(config)# remote-admin web primary-port enable`	Enable remote web admin.

Restore Factory Defaults

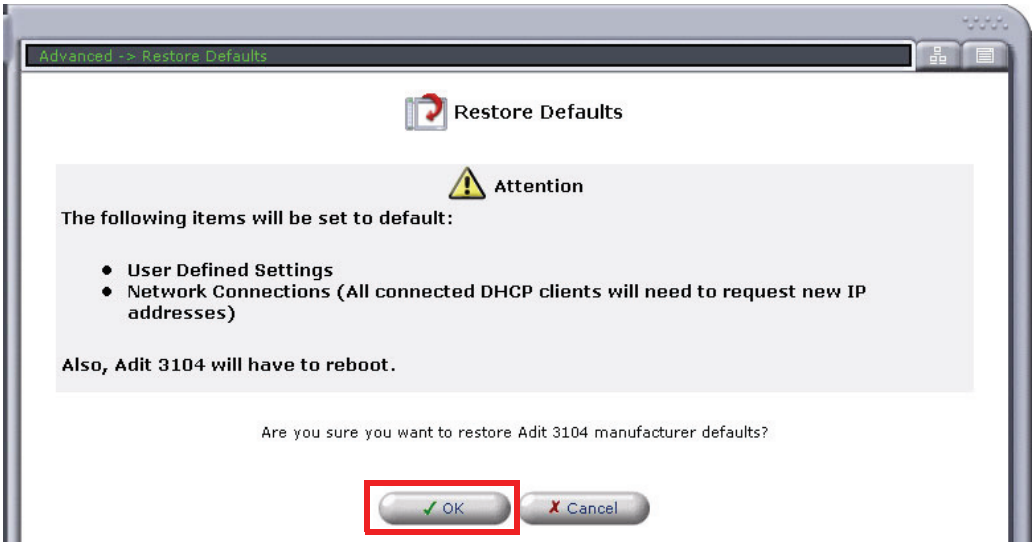
If the unit is not out-of-the-box, you may want to verify that the unit is set to defaults. Note: This will reset the IP address back to the default setting of 192.168.1.1.

In the web-browser:

- Select **Advanced** from the Navigation bar
- Select **Restore Defaults**



- Select **OK** to restore defaults


Advanced -> Restore Defaults
Restore Defaults
Attention
The following items will be set to default:
User Defined Settings
Network Connections (All connected DHCP clients will need to request new IP addresses)
Also, Adit 3104 will have to reboot.
Are you sure you want to restore Adit 3104 manufacturer defaults?
OK
Cancel

Modify Default Admin User

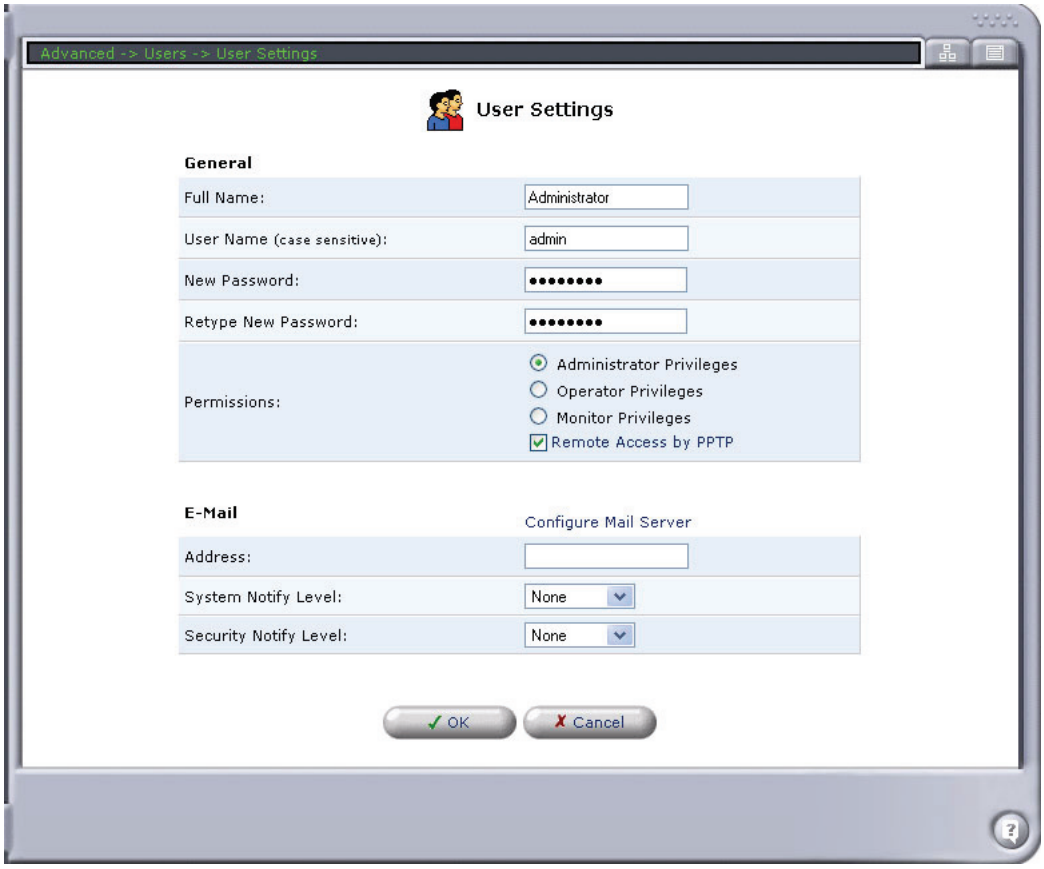
For security purposes it is recommended that the Administrator User be changed from the default settings.

Modify the Administrator User in the web-browser:

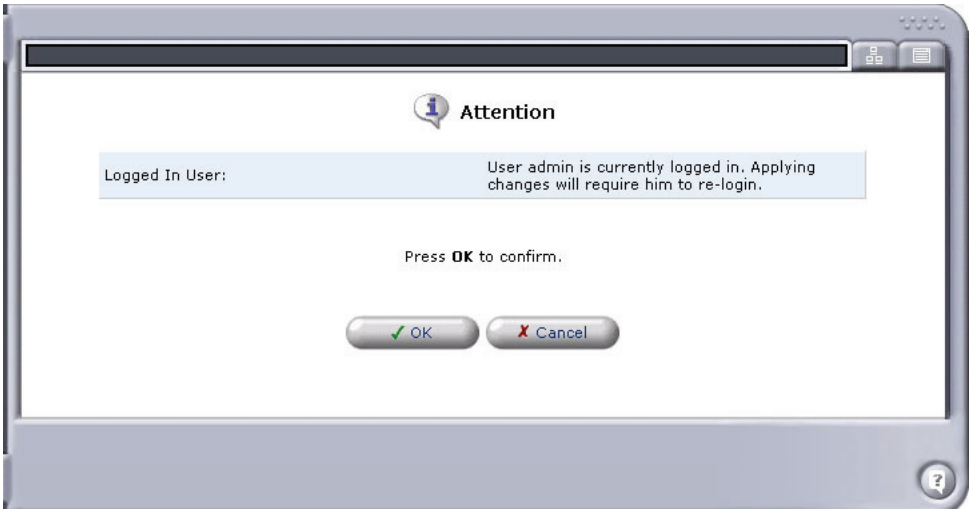
- Select **Advanced** from the Navigation bar
- Select **Users** icon

- Select **Administrato**r, to open the profile.

- Modify the User information, and select **OK** to save. It is important to note that you need to have a minimum of one user with **Administrative Privileges**. For users with other access levels, add a **New User**.
  Note: For security purposes, the password should be changed.



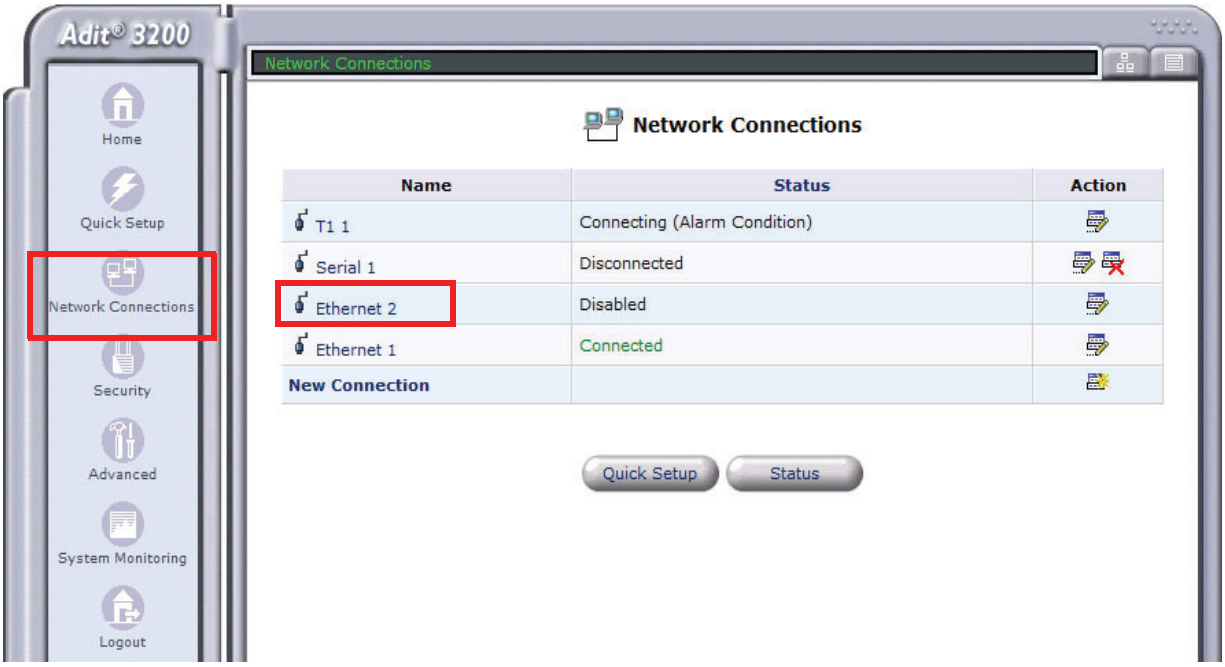
- You will be required to login again, if you have modified the User Profile that you are logged in with.



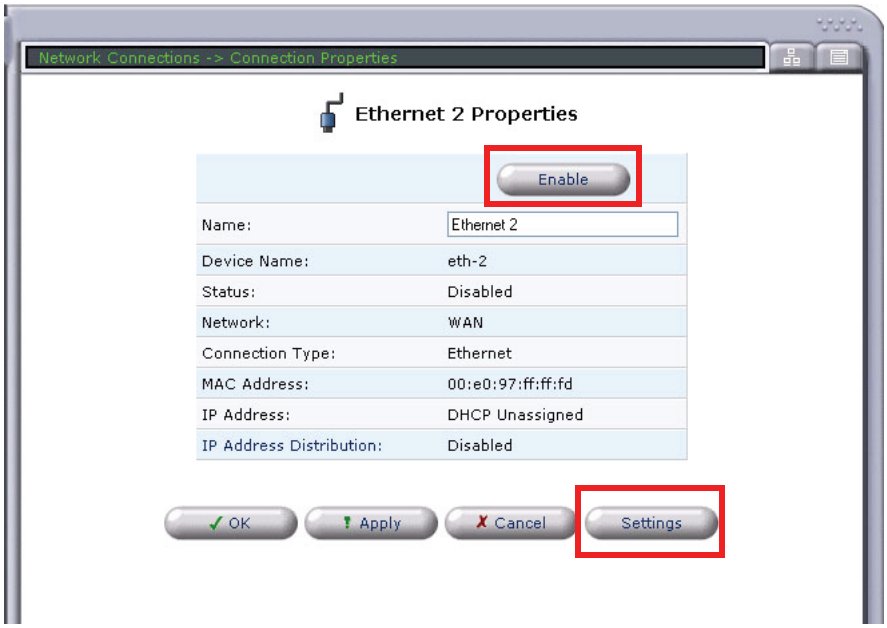
Configure Ethernet WAN Interface

In the web-browser:

1. Select **Network Connections** from the Navigation bar.
2. It is recommended that you disable/delete the Serial1 port.
3. Select (click) **Ethernet 2** (WAN Ethernet) connection to configure.



4. Select the **Enable** button, to configure the WAN Ethernet up (or in-service).
5. Select the **Settings** button.



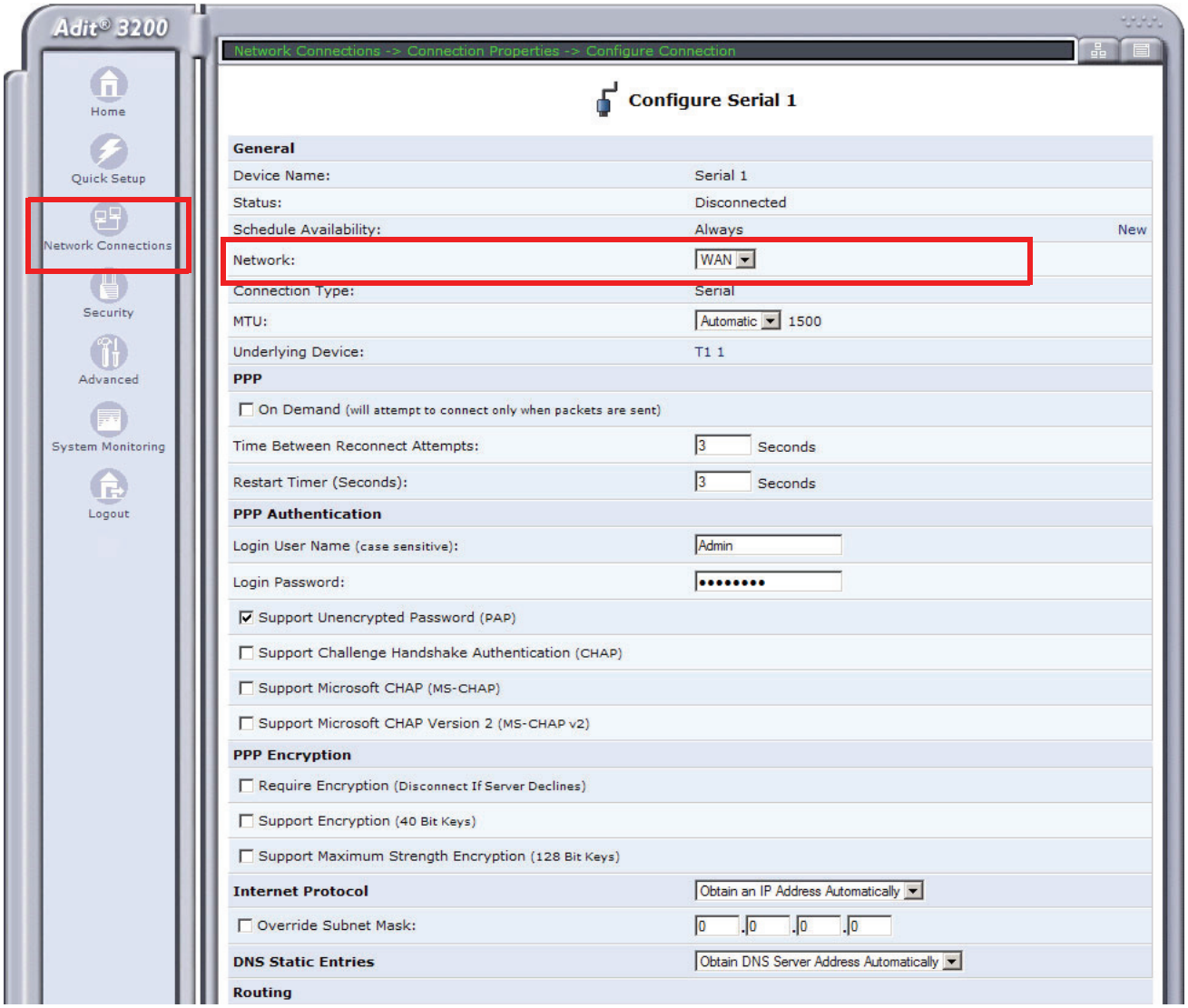
6. Set **Internet Protocol** to **Obtain an IP Address Automatically**, from the pulldown menu. This will enable the Adit 3200 as a DHCP Client. Leave the other fields to their default settings.

7. Select **Apply** to apply the new settings.

Configure Serial 1 as WAN

In the web-browser:

1. Select **Network Connections** from the Navigation bar.
2. Select **Serial 1**.
3. Select **Settings** button.
4. Set **Network** to **WAN**.
5. Select **Apply** to apply the new settings.



GLOSSARY

AMI	Automatic Mark Inversion
ARP	Address Resolution Protocol
B8ZS	Bipolar with 8 Zero Substitution
BIT	Binary Digit
BPS	Bits Per Second
BPV	Bipolar Violation
CA	Certificate Authority
CAS	Channel Associated Signaling
CCS	Common Channel Signaling
CHAP	Challenge Handshake Authentication Protocol
CID	Caller ID
CIDR	Classless Inter-Domain Routing
CLASS	Custom Local Area Signaling Service
CLEI	Common Language Equipment Identification
CLI	Command Line Interface
CO	Central Office
CPD	Calling Party Disconnect
CPE	Customer Provided Equipment
CRC	Cyclic Redundancy Check
CRV	Call Reference Value
CSU	Channel Service Unit
dB	decibel
DCS	Digital Signal Processor
DDNS	Dynamic Domain Name System
DDS	Digital Data Service
DLC	Digital Loop Carrier

DLCI	Data Link Connection Identifier
DMZ	Demilitarized Zone
DNS	Domain Naming System
DS0	Digital Signal Level Zero (64 kbps) (1 voice channel)
DS1	Digital Signal Level 1 (1.544 Mbps)
DSU	Digital Service Unit/Data service Unit
DTE	Data Terminal Equipment
DTMF	Dual Tone Multi-Frequency
ES	Errored Seconds
ESF	Extended Superframe
FDL	Facilities Data Link
FXS	Foreign Exchange Station
GS	Ground Start
HDB3	High Density Bipolar 3
IP	Internet Protocol
IPX	Internet Packet eXchange
ISDN	Integrated Services Digital Network
LAN	Local Area Network
LAPD	Link Access Procedure on the D channel status
LBO	Line Build Out
LLC	Logical Link Control
LMI	Local Management Interface
LS	Loop Start
LULT	Line Unit Line Termination
Mbps	Million Bits Per Second
MLPPP	Multilink PPP
MPPE	Microsoft Point-to-Point Encryption
MS-CHAP	Microsoft CHAP
MVEC	Majority Vote Error Correction

NAT	Network Address Translation
NCS	Network-based Call Signaling
NEBS	Network Equipment Building Standards
NRZ	Non-Return to Zero
NSE	Named Service Event
NTP	Network Time Protocol
OSPF	Open Shortest Path First
PAP	Password Authentication Protocol
PHY	Physical specifications
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PRI	Primary Rate Interface
PVC	Permanent Virtual Circuit
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In Service
SABME	Set Asynchronous Balanced Mode Extended
SDP	Session Description Protocol
STP	Spanning Tree Protocol
T1	Trunk Level 1 (1.544 Mbps)
TDM	Time Division Multiplex
TEI	Terminal Endpoint Identifier
TFTP	Trivial File Transfer Protocol
TOS	Type of Service
UAC	User Agent Client
UAS	User Agent Server
VC	Virtual Channel
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

WAN	Wide Area Network
WINS	Windows Internet Naming Service

10Base-T	The most widely installed Ethernet local area networks (LANs) use ordinary telephone twisted-pair wire. When used on Ethernet, this carrier medium is known at 10BASE-T. 10BASE-T supports Ethernet's 10 Mbps transmission speed.
100Base-TX	Also called "Fast Ethernet", it is a 100 Mbps version of Ethernet. 100Base-T transmits at 100 Mbps rather than 10 Mbps. Like regular Ethernet, Fast Ethernet is a shared media LAN. All nodes share the 100 Mbps bandwidth. 100Base-TX uses two pairs of Category 5 cabling, one pair for transmission, one pair for receiving.
Address Resolution Protocol (ARP)	An internet protocol used to map dynamic internet addresses to physical addresses on Local Area Networks.
analog	The telephone transmission of voice, video or image. Telephone transmission and/or switching that is not digital.
Asynchronous Transfer Mode (ATM)	Very high speed transmission technology. ATM is a high bandwidth, low-delay, connection-oriented, packet-like switching and multiplexijng technique. Usable capacity is segmented into 53-byte fixed-size cells, consisting of header and information fields, allocated to services on demand. The term "asynchronous" applies, as each cell is presented to the network on a "start-stop" basis - in other words, asynchronously.
authentication	The process of identifying an individual, usually based on a username and password combination, although the process can be many more steps. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual. Authentication in whatever form, is usually followed by authorization.
bandwidth	The width of a communications channel. Analog is typically measured in Hertz (cycles per second), a voice conversation is typically measured in bits per second.
Basic Rate Interface (BRI)	Basic Rate Interface (2b+d) in ISDN.
Bipolar 8-Zero Substitution	A coding scheme that maintains ones density.
bipolar violation	BPV. A violation is declared for AMI if two successive pulses have the same polarity.
bit	Contraction of the words "binary" and "digit".
Bit Error Rate	The number of erred bits divided by the total number of bits.
broadband	A technology that provides an extremely wide and fast bandwidth so that many people can simultaneously use the service. It is generally associated with multiple types of transmissions on the same connection such as voice, data, video and digital or analog information.
Central Office (CO)	Where telephone companies terminate customer lines and locate switching equipment to interconnect those lines with other networks.

channel	A generic term for a communications path on a given medium; multiplexing techniques allow providers to put multiple channels over a single medium.
Channel Associated Signaling (CAS)	Carrying signaling information within the data channels of a T1 line (in band) rather than on a separate control channel. CAS signaling is also used to carry 911 emergency data such as telephone number and location information.
Channel Service Unit (CSU)	The interface to the T1 line that terminates the local loop.
Classless Inter-Domain Routing	CIDR is a new addressing scheme for the Internet which allows for more efficient allocation of IP addresses than the old Class A, B, and C address scheme.
CLEI Codes	Common Language Equipment Identifier codes, that are assigned by Bellcore to provide a standard method of identifying telecommunications equipment in a uniform, feature-oriented language.
CLI	Command Line Interface
collision	In Ethernet, the result of two nodes transmitting simultaneously. The frames from each device impact and are damaged when they meet on the physical media.
command line	The command line is where you enter MS-DOS commands.
compander	Companding is the process of compressing the amplitude range of a signal for economical transmission and then expanding them back to their original form at the receiving end.
Demilitarized Zone (DMZ)	A collection of computers that are shielded from both the trusted network and the untrusted network by packet-filtering routers and gateways.
Domain Naming System (DNS)	DNS. A mechanism used in the Internet for translating names of host computers into addresses.
download	To transfer data from a larger “host” system to a smaller “client” system's hard drive or other local storage device.
Dual Tone Multi-Frequency (DTMF)	Dual Tone Multi-Frequency is a term describing push button or Touchtone dialing.
Dynamic Domain Name System (DDNS)	Allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (e.g., www.xyz.com) and a dynamic IP address.
Dynamic Host Configuration Protocol (DHCP)	DHCP is a network configuration that allows maintenance to be performed from a central site rather than by end users.
Earth ground	A wire conductor that terminates in the earth for electrical purposes. It is generally the negative side of the circuit and is most important in alternating current (AC) circuits. Chassis Ground is the general term used in direct current (DC) circuits.

Electro-magnetic Interference (EMI)	Equipment used in high speed data systems, including ATM, that generate and transmit many signals in the radio frequency portion of the electromagnetic spectrum. Interference to other equipment or radio services may result if sufficient power from these signals escape the equipment enclosures or transmission media. National and international regulatory agencies (FCC, CISPR, etc.) set limits for these emissions. Class A is for industrial use and Class B is for residential use.
Ethernet	Ethernet is a particular network topology and protocol, especially useful in LANs. It comes in various speeds and is often regarded as THE current technology for general network direct connection. The current connectivity is generally considered to be 10Base-T or 100Base-T, while the backbone, if one is used, is coaxial cable or Fiber optics. There is also a 1000Base-T for certain specialty copper joining situations.
Facilities Data Link (FDL)	FDL supports the communication of various network information in the form of in-service monitoring and diagnostics.
filter	An operating parameter used with routers that can be set to block the transfer of packets from one LAN to another.
firewall	Any of a number of security schemes that prevent unauthorized users from gaining access to a computer network and/or may monitor the transfer of information to and from the network.
frame	A fragment of data that is packaged into a frame format, which comprises a header, payload, and trailer.
Frame Reject (FRMR)	The FRMR response frame is sent to report the receiver of a frame cannot successfully process that frame and that the error condition is not correctable by sending the offending frame again.
Foreign Exchange	A Central Office trunk which has access to a distant central office. Dial Tone is returned from that distant Central Office, and a location can be reached in the area of the foreign Central Office by dialing a local number. This will provide easier access for customers in that area and calls may be made anywhere in the foreign exchange area for a flat rate.
Foreign Exchange Service	Foreign exchange (FX) service is a service that can be ordered from the telephone company that provides local telephone service from a central office which is outside (foreign to) the subscriber's exchange area. Simply, a user can pick up the phone in one city and receive a dial tone in the foreign city. This kind of connection is provided by a type of trunk called foreign exchange (FX) trunk. FX trunk signaling can be provided over analog or T-1 links. Connecting POTS telephones to a computer telephony system via T-1 links requires a channel bank configured with FX type connections.
G.711	ITU-T Recommendation for an algorithm designed to transmit and receive A-law and mu-law PCM voice at digital bit rates of 48, 56, and 64 Kbps. It is used for digital telephone sets on digital PBX and ISDN channels.
G.729	International Telecommunications Union's standard voice algorithm (CS-ACELP) voice algorithm for the coding of encoding/decoding of speech at 8 Kbps using conjugate-structure, algebraic-code excited linear predictive methods. Described in the ITU-T standard in its G-series recommendations.

gateway	An entrance and exit into a communications network
Graphical User Interface (GUI)	GUI, pronounced "GOOEY". A set of screen presentations and metaphors that utilize graphic elements such as icons in an attempt to make an operating system easier to use.
ground	A physical connection to the earth or other reference point.
ground start (GS)	A method of signaling on subscriber trunks in which one side of the two wire trunk (typically the ring conductor of Tip and Ring) is momentarily grounded to get dial tone.
hash algorithm	A one way function that takes an input message of arbitrary length and produces a fixed length digest. Adit uses both Secure Hash Algorithm (SHA) and Message Digest 5 (MD5) hashes within our implementation of the IPSec framework.
High Density Bipolar 3	HDB3. A bipolar coding method that does not allow more than 3 consecutive zeros.
hop	Each individual short trip that packets make from router to router, as they are routed to their destination.
host	A computer that allows users to communicate with other host computers on a network.
impedance	The total opposition a circuit offers to the flow of alternating current. It is measured in ohms and the lower the ohmic value, the better the quality of the conductor
internet	"A network of networks," the Internet supports FTP, WWW, Gopher, E-Mail, Telnet, and many other world-wide information transfer protocols and services. ISPs provide an effective interface with the Internet. The Internet itself is made up of thousands of LANs and WANs, all using TCP/IP to provide information services to millions of users. A worldwide network of networks that all use the TCP/IP communications protocol and share a common address space.
Internet Protocol (IP)	Internet Protocol, the method by which most Internet activity takes place. Members with access to TCP/IP through a SLIP or PPP connection can connect to many ISP services in this manner. As the name implies, it is a protocol for network activity. Most current networks support some sort of TCP or IP directly or indirectly.
IP address	A string of four numbers separated by periods (such as 111.22.3.144) used to represent a computer on the Internet. The format of the address is specified by the Internet Protocol in RFC 791. Each of the four number must be 255 or less; they may be 0.
IPSec	IPSec (IP Security) is a set of IP extensions developed by IETF to provide security services compatible with the existing IP standard (IPv.4) and also the upcoming one (IPv.6). In addition, IPSec can protect any protocol that runs on top of IP, for instance TCP, UDP, and ICMP. The IPSec provides cryptographic security services. These services allow for authentication, integrity, access control, and confidentiality. IPSec allows for the information exchanged between remote sites to be encrypted and verified. You can create encrypted tunnels (VPNs), or just do encryption between computers.
jitter	Interference on an analog line caused by a variation of a signal from its reference timing slots. Jitter can cause problems in the receipt of data and any subsequent processing of that data.

Local Area Network (LAN)	A short distance data communications network (typically within a building or campus) used to link together computers and peripheral devices under some form of standard control.
Line Build Out (LBO)	T1s require the last span to lose 15 - 22.5 dB, a selectable output attenuation is generally required of DTE equipment.
Line Coding Violation (LCV)	This parameter is a count of both BPVs and EXZs occurring over the accumulation period. An EXZ increments the LCV by one regardless of the length of the zero string.
Line Errored Seconds (LES)	A Line Errored Second is a second in which one or more CVs occurred OR one or more LOS defects.
Local Link Control (LLC)	A protocol developed by the IEEE 802.2 committee for data-link-level transmission control
Local Management Interface	A specification for the use of frame-relay products that define a method of exchanging status information between devices such as routers
loop start (LS)	A method of demanding dial tone from the central office by completing an electrical pathway between the outbound and return conductors of a telephone line. Loop start is employed by single-line telephone instruments, for example
loopback	A diagnostic test in which a signal is transmitted across a medium while the sending device waits for its return.
MAC Address	The address for a device as it is identified at the Media Access Control layer in the network architecture
Management Information Base (MIB)	A data base of objects, with attributes and values, representing the manageable components of a network device. Used in SNMP. There are industry standardized MIBs and proprietary MIBs
mapping	In network operations, the logical association of one set of values, such as addresses on one network, with quantities or values of another set, such as devices on another network.
Media Access Control (MAC)	The lower of the two sub-layers of the data link layer defined by the IEEE. The MAC sub-layer handles access to shared media, such as whether token passing or contention will be used. The MAC contains the standardized data link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are 6 bytes long and are controlled by the IEEE.
Multilink PPP (MLPPP)	MultiLink PPP. An extension to the point-to-point protocol that enables two channels to be linked together to double the throughput. It is used for ISDN transmission and channel bonding
Microsoft Point-to-Point Encryption (MPPE)	A 128-bit key or 40-bit key encryption algorithm using RSA RC4. MPPE provides for packet confidentiality between the remote access client and the remote access or tunnel server and is useful where IP security (IPSec) is not available. MPPE 40-bit keys are used to satisfy current North American export restrictions. MPPE is compatible with Network Address Translation.

modem	MOdulator-DEModulator, a device that takes digital computer signal, converts it to analog, and sends it across the phone line. Another modem on the reverse does the exact opposite action. Modems transfer data at different speeds or rates, called baud.
multiplexer	Electronic equipment which allows two or more signals to pass over one communications circuit. The circuit may be analog or digital
MUX	See multiplexer
NetBIOS	Network Basic Input/Output System.NetBIOS is a program that allows applications on different computers to communicate within a Local Area Network (LAN).
network	A set of computers linked to one another for data sharing, or the link itself.
Network Time Protocol (NTP)	Network Time Protocol, developed to maintain a common sense of time among Internet hosts around the world. Many systems on the Internet run NTP, and have the same time (relative to Greenwich Mean Time).
Non-Return to Zero (NRZ)	A binary encoding scheme in which ones and zeros are represented by opposite and alternating high and low voltages and where there is no return to a zero (reference) voltage between encoded bits.
Open Shortest Path First (OSPF)	Short for Open Shortest Path First, an interior gateway routing protocol developed for IP networks based on the shortest path first or link-state algorithm. Routers use link-state algorithms to send routing information to all nodes in an internetwork by calculating the shortest path to each node based on a topography of the Internet constructed by each node. Each router sends that portion of the routing table (keeps track of routes to particular network destinations) that describes the state of its own links, and it also sends the complete routing structure (topography). The advantage of shortest path first algorithms is that they results in smaller more frequent updates everywhere. They converge quickly, thus preventing such problems as routing loops and Count-to-Infinity (when routers continuously increment the hop count to a particular network). This makes for a stable network. Note: OSPF Version 2 is defined in RFC 1583. It is rapidly replacing RIP on the Internet.
packet	A packet consists of the data to be transmitted and certain control information.
PAP	Password Authentication Protocol
PAT	Port Address Translation
PHY	PHY as in physical specifications. OSI Physical Layer, which provides for transmission of cells over a physical medium connecting two ATM devices.
ping	Packet InterNet Grouper. PING is a program used to test whether a particular network destination on the Internet is online (i.e. working) by repeatedly bouncing a "signal" off a specified address and seeing how long that signal takes to complete the round trip. No return signal - site is down or unreachable. Portion is returned - trouble with the connection.
PLAR	Private Line, Automatic Ringdown. A leased voice circuit that connects two single instruments together. When either handset is lifted, the other instrument automatically rings.

PPP	Point-to-Point Protocol. is used for establishing a point-to-point link that provides a single, preestablished WAN communications path from the customer premises, through a carrier network (the telephone company), to a remote network
PPPoT1	Point-to-Point over T1.
PRACK	Provisionable acknowledgement.
Primary Rate Interface (PRI)	The ISDN equivalent of a T1. The Primary Rate Interface (delivered to the customer's premise) provides 23B+D (N.America) or 30B+D (Europe) running at 1.544 Mb/sec and 2.048 Mb/sec, respectively.
protocol	Procedure or set of rules.
PVC	Permanent Virtual Circuit. A PVC is a permanent channel connection between two ATM devices. PVC's allow network transmissions to be started without having to first establish a connection with the end point ATM device. When a PVC is constructed, the end points of the connection will agree upon a path in which data will travel, and therefore agree upon the route that data will travel to reach its destination.
Quality of Service (QoS)	The measure of the telephone service quality provided to a subscriber.
RADIUS	Remote Authentication Dial-In Service. RADIUS is a client/server-based authentication software system. The software supports remote access applications, allowing an organization to maintain user profiles in a centralized database residing on an authentication server which can be shared by multiple remote access servers.
robbed bit	A type of analog signaling that will occasionally steal information bits used for circuit signaling coding.
router	A computer or internet working device that directs traffic and moves packets between networks. A hardware architecture used in LANs, MANs, WANs, the Internet and Intranets. A device that connects any number of LANs. Routers use headers and a forwarding table to determine where packets go, and they use ICMP to communicate with each other and configure the best route between any two hosts.
Router Information Protocol (RIP)	RIP is based on distance vector algorithms that measure the shortest path between two points on a network, based on the addresses of the originating and destination devices. The shortest path is determined by the number of hops between those points. Each router maintains a routing table, or routing database, of known addresses and routes; each router periodically broadcasts the contents of its table to neighboring routers in order that the entire network can maintain a synchronized database.
Router Information Protocol Version 1 (RIPv1)	Original version of RIP. This is a classful routing protocol, it does not have the ability to transmit the subnet mask within its updates. RIP v1 imposes the subnet mask on the inbound interface and this is normally defined by the engineer. Learned routes are entered into the routing table with their natural mask. As a result there can be a great waste of internet host addresses.
Router Information Protocol Version 2 (RIPv2)	Second version of RIP, additional to Version 1, enables the use of a simple authentication mechanism to secure table updates. More importantly, RIP 2 supports subnet masks, a critical feature that is not available in RIP (v1).

SAP	Service Access Point.
signal	A generated electrical impulse that is a change in voltage to trigger an event.
Simple Network Management Protocol (SNMP)	SNMP is the most common method by which network managements applications can query a management agent using a supported MIB (Management Information Base). SNMP operates at the OSI application layer.
spanning tree	Spanning Tree Protocol is a link management protocol that provides path redundancy while preventing undesirable loops in the network. For an Ethernet network to function properly, only one active path can exist between two stations.
SRV	SRV is an resource record that specifies the locations of servers.
subnet mask	32-bit quantity indicating which bits in an IP address identify the physical network
T1	Trunk Level 1. A digital transmission link with a total signaling speed of 1.544 Mbps. T-1 is a standard for the digital transmission in North America.
telnet	An Internet standard protocol that enables a computer to function as a terminal working from a remote computer
TDM	Time Division Multiplex. A technique for transmitting a number of separate data, voice and/or video signals simultaneously over one communications medium by quickly interleaving a piece of each signal one after another.
Terminal Endpoint Identifier (TEI)	Up to eight devices can be connected to one ISDN BRI (or PRI) line. The TEI defines, for a given message, which of the eight devices is communicating with the Central Office switch. In general, more than one of the eight may be communicating.
TFTP	Trivial File Transfer Protocol.
ticks	The distance between two networks, measured in time increments. Ticks may be used to designate primary and secondary routes to the same network.
traffic	The load of packets carried by a network or portion of a network. Heavy traffic slows down the response time of the individual packets.
trunk	A communication line between two switching systems.
tunneling	To provide a secure, temporary path over the Internet.
V.90	The standard for full-duplex modems sending and receiving data across phone lines at up to 56,600 bps, approved by the International Telecommunication Union (ITU) in February, 1998.
Virtual Private Network (VPN)	A software defined network offering the appearance, functionality and usefulness of a dedicated private network, at a price savings.
VC MUX	Virtual Channel Multiplexer

Wide Area Network (WAN)	A private long distance network that uses leased lines to connect computers or LANs. A wide area network is a linking of computers not physically attached through conventional network connectivity. Usually the WAN connection is a dedicated or high grade dial up phone link. It is often done with T1 or T3 connections but can also be through satellite or other technologies.
WINS	Windows Internet Naming Service. A system that determines the IP address associated with a particular network computer.
Virtual Connection (VC)	A connection between two hosts in a packet-switching network. In this case, the two hosts can communicate as though they have a dedicated connection even though the packets might actually travel very different routes before arriving at their destination.
Virtual Local Area Network (VLAN)	A VLAN consists of a network of computers that behave as if connected to the same wire, though they may actually be physically connected to different segments of a LAN. VLANs are configured through software rather than hardware, which makes them extremely flexible.

INDEX

Numerics

100Base-T 3-3

A

AC Power (Adapter) 3-4
Adit 3000
  base platform 1-1
  chassis 1-6
  overview 1-2
  technical specifications 1-3
Alarm LEDs 3-8
all modes
  key 4-7
altitude 2-2

B

Base Platform
  technical specifications 1-3

C

chassis 1-6
  dimensions 1-5
CLI command
  key 4-7
CLI connection 4-5
Compliant Installation 2-3
Configuration
  PC Network Configuration 4-2
connectors
  DB-9 3-5
  interface 3-3
  RS-232 3-5

D

dimensions 1-5
DS1
  connector pinout 3-6
  LEDs 3-6

E

Electrical
  cabling 3-1
  installation 3-1
Environment Requirements
  non-operating altitude 2-2
  operating altitude 2-2
  operating temperature 2-2
  relative humidity 2-2
  storage temperature 2-2
Ethernet 3-3
  connector pinout 3-7

F

feature keys 4-7
fuse recommendations 3-4

G

Grounding the unit 3-3

H

humidity 2-2

I

Installation Environment 2-2
  non-operating altitude 2-2
  operating altitude 2-2
  operating temperature 2-2
  relative humidity 2-2
  storage temperature 2-2
interface
  connectors 3-3

K

Key enabled Features 4-7
keys, feature 4-7

L

LEDs
  Alarm 3-8
  DS1 3-6
  Status 3-8
  T1 3-6
Login 4-6

M

mounting
  rack 2-6
  wall bracket 2-5

N

non-operating altitude 2-2

O

operating
  altitude 2-2
  temperature range 2-2

P

PC Network Configuration 4-2
Physical Information 1-5
pinouts
  DB-9 3-5
  RJ-48C 3-6
Power 3-4
  AC Power (Adapter) 3-4

R

rack mounting 2-6
relative humidity 2-2
RJ-45 pinout 3-7
RJ-48C 3-3
RS-232 . . . . . 3-3, 4-5
  connector pinout 3-5

S

Status LED 3-8
storage temperature range 2-2
system overview 1-2

T

T1
  connector pinout 3-6
  LEDs 3-6
technical specifications 1-3
temperature requirements 2-2

U

Unpacking and Inspection 2-2

W

wall mounting 2-5
weight 1-5